2005-12

Identity theft prevention in CyberCIEGE

Ruppar, Carrie Aliene

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IDENTITY THEFT PREVENTION IN CYBERCIEGE

by

Carrie Aliene Ruppar

December 2005

Thesis Co-Advisors:	Cynthia E. Irvine
	Paul C. Clark
Second Reader:	Michael F. Thompson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Identity Theft Prevention in CyberCIEGE			**5. FUNDING NUMBERS**
6. AUTHOR(S) Carrie Aliene Ruppar			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The increase in online activities which involve people's identification information means that identity theft has become a widespread computer security issue. Identity theft is defined as the misuse of personal information and identity. To address this problem, an Information Assurance training tool, such as CyberCIEGE, can be used for user awareness and education.

This thesis incorporated current research on identity theft attacks and prevention techniques into a customized scenario definition file for the CyberCIEGE game engine. The scenario teaches players about methods of identity theft prevention in computing and networked environments by focusing on four main prevention techniques: updating antivirus protection regularly, being cautious about executable email attachments, resisting phishing attacks, and using secure web browser connections for online transactions. After scenario development, an informal test process of the Identity Theft scenario was conducted. Testing found that the experienced and expected results coincided. Recommendations for improvement of the CyberCIEGE game engine, Scenario Definition Tool, and Identity Theft scenario were also provided.

14. SUBJECT TERMS Identity Theft Prevention, Computer Security, Information Assurance, Social Engineering, CyberCIEGE, Scenario Definition File, Training			**15. NUMBER OF PAGES** 54
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IDENTITY THEFT PREVENTION IN CYBERCIEGE

Carrie A. Ruppar
Civilian, Naval Postgraduate School
B.A., Wellesley College, 2000
M..A., University of Texas-Austin, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCEINCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2005

Author: Carrie Aliene Ruppar

Approved by: Dr. Cynthia E. Irvine
Thesis Co-Advisor

Paul C. Clark
Thesis Co-Advisor

Michael F. Thompson
Second Reader

Dr. Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The increase in online activities which involve people's identification information means that identity theft has become a widespread computer security issue. Identity theft is defined as the misuse of personal information and identity. To address this problem, an Information Assurance training tool, such as CyberCIEGE, can be used for user awareness and education.

This thesis incorporated current research on identity theft attacks and prevention techniques into a customized scenario definition file for the CyberCIEGE game engine. The scenario teaches players about methods of identity theft prevention in computing and networked environments by focusing on four main prevention techniques: updating antivirus protection regularly, being cautious about executable email attachments, resisting phishing attacks, and using secure web browser connections for online transactions.

After scenario development, an informal test process of the Identity Theft scenario was conducted. Testing found that the experienced and expected results coincided. Recommendations for improvement of the CyberCIEGE game engine, Scenario Definition Tool, and Identity Theft scenario were also provided.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis team, Dr. Cynthia Irvine, Paul Clark, and Mike Thompson. I really appreciate all of your support and guidance during the entire process.

I would also like to thank all of those involved in the Federal CyberCorps/Scholarship for Service Program, both nationally and at the Naval Postgraduate School. I am very grateful for the opportunity to be a part of the program and attend the Naval Postgraduate School.

I would also like to thank Richard Riehle. You have been a great mentor and friend. Thank you for challenging, supporting, and inspiring me.

This material is based upon work supported by the National Science Foundation under Grant No DUE-0114018 and by the Office of Naval Research. I would like to thank the National Science Foundation and the Office of Naval Research for their contributions. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation or of the Office of Naval Research..

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

Identity theft is a widespread computer security issue which needs to be addressed through user awareness and training. To speak to this need, this thesis incorporates current research on identity theft attacks and prevention techniques into a customized scenario definition file for the CyberCIEGE game engine. The scenario will serve to teach players about methods of identity theft prevention in computing and networked environments.

B. THESIS ENVIRONMENT

In both the corporate and government environments, employees are often required to undergo informational and user training sessions. For example, new employees undergo orientation on policies such as the company's password policy, computer usage policy, or security policy. Traditional orientation methods of sitting in a room and verbally going over all the information may cause users to feel inundated and overwhelmed. This can cause the important security information to be lost in the shuffle. However, by developing new methods of training, such as simulation games or educational tools, companies can provide a more engaging learning experience for their employees. "By capturing students' imaginations and generating a sense of competition, games provide a stimulating environment in which the participant has a stake in the outcome" (Irvine, Thompson, and Allen 2005, 61). Also, by having alternative training techniques, companies will be able to cater to different learning styles. For example, a visual learner would benefit from being trained with CyberCIEGE because they can see the concepts in action.

The Center for Information Systems Studies and Research (CISR) at the Naval Postgraduate School is currently developing CyberCIEGE, a DOD educational tool developed to train users in Information Assurance concepts in a virtual environment. "CyberCIEGE consists of several elements: a simulation engine, a scenario-definition language, a scenario-development tool, and a video-enhanced encyclopedia" (Irvine,

Thompson, and Allen 2005, 62). In any given scenario, a CyberCIEGE player is presented with a budget and must make security-related decisions to help the virtual user achieve his or her objectives and be productive. If goals are not achieved, the player will encounter consequences, such as financial penalties. Poor security decisions lead to compromised assets. "Using the potential tension between strong security and user productivity, CyberCIEGE illustrates that many security choices are an exercise in risk management" (Irvine, Thompson, and Allen 2005, 61).

This thesis expanded the current training suite by providing the player with an identity theft scenario. It deviates from the existing scenarios by being set in the user's home versus a workplace environment. This scenario trains home computer users about how they should configure and operate their personal computers to prevent identity theft. The techniques and concepts of identity theft prevention presented in the scenario can be applied to any computing environment.

C. THESIS OVERVIEW

Research about current prevalent identity theft attacks was conducted and analyzed in order to develop the CyberCIEGE scenario. In the scenario, the player configures a personal computer to be protected from identity theft attacks by selecting various configuration settings. The player attempts to influence the behavior of a virtual user through various procedural policy settings. After scenario development, a test plan was constructed to identify the means of testing the scenario. Test goals included whether or not the scenario definition file worked properly and successfully conveyed identity theft prevention techniques. Specific test cases were defined in terms of anticipated player choices and expected results. The final scenario was run against these test cases.

The thesis is divided into chapters as follows:

I. Introduction - This chapter discusses the scope, environment, and outline of the thesis.

II. Identity Theft - This chapter provides the motivation behind the scenario development by highlighting research about the current threats and methods of prevention of identity theft.

III. Scenario Overview - This chapter depicts the developed scenario in detail by describing the storyline and scenario components, such as zones, assets, users, objectives, and feedback. This chapter also provides context to the scenario by discussing the intended audience and educational goals of the scenario.

IV. Testing - This chapter describes the testing process in terms of the test strategy and test cases. It also discusses the testing of the CyberCIEGE game engine and Scenario Definition Tool.

V. Conclusion - This chapter provides insights of how this thesis could be extended in the future and recommendations for improving the CyberCIEGE game engine and Scenario Definition Tool.

THIS PAGE INTENTIONALLY LEFT BLANK

II. IDENTITY THEFT

A. WHAT IS IDENTITY THEFT?

Identity theft has become such a prevalent threat to our security that the subject matter pervades current popular culture. Movies such as *The Net; Single, White, Female;* and *Catch Me If You Can* speak to the dangers of what can happen when our personal information falls into the wrong hands. Credit card commercials exist that attempt to use humor to raise the public's awareness of the dangers of identity theft. Storylines in popular television shows, such as *General Hospital*, also represent this rise in public awareness of identity theft. Yet despite the fact that identity theft has become a part of society's vocabulary, information on how to prevent and protect ourselves from identity theft has yet to become as pervasive.

Identity theft is defined as the "misuse of a another person's identity, such as name, social security number, driver's license, credit card numbers, and bank account numbers" (Denning 1999, 241). A victim's personal information can be used for both financial gain and to physically misrepresent the victim to people such as law enforcement officials, employers or medical providers. According to a 2003 survey by the Federal Trade Commission, identity theft fraud can be broken down into three main types of misuse: new accounts and other fraud, misuse of existing non-credit card accounts or account numbers, and misuse of existing credit cards or credit card numbers. The Federal Trade Commission found that "almost 10 million Americans have discovered that they were the victim of some form of ID Theft within the last year," and that the number of victims is increasing every year (Synovate 2003, 4). The amount of time associated with resolving the problems that arise in the aftermath of identity theft should also be considered a cost of identity theft. In 2003, "Americans spent almost 300 million hours resolving problems related to ID Theft in the past year" (Synovate 2003, 6).

Not only does identity theft impact the consumer, but it also negatively affects business and banks. The Federal Trade Commission estimated that the loss to businesses and banks totaled around thirty-three billion dollars in 2003 (Synovate 2003, 6). Businesses and financial institutions have had to keep up with the increase in identity

theft by developing new services. For example, most credit card providers now provide the option of placing the credit card owner's picture on the credit cards for authentication purposes. Similarly, since monitoring one's credit report is a commonly recommended technique to prevent identity theft, some financial institutions now allow consumers to buy identity theft prevention each month through special credit checking services. Identity theft is a costly threat which needs to be addressed in one way or another.

B. THREATS

"The greatest threat to security is not privacy but convenience" (Caloyannides 2004, 84). Services such as paying bills, banking, stock trading, and purchasing products are now becoming more prevalent online. On the outside of the return envelopes, telephone and electric companies, such as SBC and PG&E, are encouraging their customers to receive and pay their bills online. The Federal Trade Commission found that 13% of their survey respondents claimed that their personal information was stolen through transactions, such as online purchasing (Synovate 2003, 31). These online services include a form of identification and authentication, usually in the form of a username and password. While making it more convenient for people to pay bills and see information about their accounts, it also leaves personal information open to cyberattacks and identity theft.

Social engineering is a key way that personal information is collected for misuse. Infosecurity Europe conducted a survey in London that found that "more than 70% of people would reveal their computer password in exchange for a bar of chocolate" (BBC News 2004). People end up becoming their own worst enemies, particularly when free items are involved. For example, stores attempt to entice consumers to sign up for store-sponsored credit cards by providing incentives and discounts at the price of personal information and a signature on an application form. Social engineering can be used directly on the individual to gain their information, as in the Infosecurity Europe survey example. But, it can also be used on companies that collect and store people's identifying information, such as department stores or credit card companies. Even if key information, such as passwords, is not supplied by the individual, enough personal information can be collected to be damaging to the security of a person's identity. It is

important to be aware of who exactly is collecting the personal information, what the information is going to be used for, and what the privacy policies are of the companies who have the information.

Poor password security and management, such as having the same password for every website a user deals with, can also cause a person to become vulnerable to identity theft. A survey conducted by VeriSign found that 79 percent of respondents "use the same password for multiple Web sites or applications" (Ostrom 2005). Another threat to personal identities is easily crackable passwords, such as names and dictionary words. Awareness of common password security techniques need to be provided to users to help alleviate these kinds of mistakes.

The need to have the latest technology can also leave one vulnerable. Centralizing information in an all-in-one device like a PDA/cell phone can make a person vulnerable if that device falls into the wrong hands. "In our love affair with new technology, it's easy to forget that our handy devices affect our privacy in more ways than we know" (Caloyannides 2004, 84). For example, the SIM (subscriber identification module) card found in some cell phones stores private information such as calls made, received, and missed, phone numbers, and photos (if the phone has a camera). Fax machines, printers, copiers, and cell phones are all devices that store information sent to them, which can then be collected later for uses not intended by the manufacturers.

People give away their contact information, date of birth, credit card number, and social security number for lots of reasons and services these days. This personal information is asked for with activities that range from buying books online to joining a professional organization to paying bills online. RSA security conducted a survey that found that "many people volunteered important personal information, such as their mother's maiden name or even their own date of birth, when questioned during a street survey" (BBC News 2004). Our view of personal information needs to shift from its use as common identifiers to data which needs to be protected and secured.

C. PREVENTION TECHNIQUES

In terms of possible solutions to the problems caused by identity theft, "many victims thought better awareness on their own part of how to prevent and respond to identity theft would have been most helpful" (Synovate 2003, 62). This thesis attempts to assist in raising computer user's consciousness about identity theft, by incorporating common prevention techniques into a CyberCIEGE scenario. Most of the recommended techniques for securing personal information on computers fall in to the realm of basic computer security practices. The following is a breakdown of the methods of prevention for digital identity theft:

1. Install and regularly update antivirus and spyware protection software. (Federal Trade Commission 2005).
2. Install and properly configure a firewall on your personal computer. (Federal Trade Commission 2005).
3. Use a secure web browser for online transactions which employs techniques, such as encryption, to keep your personal information more secure. (Federal Trade Commission 2005).
4. Do not store financial or other sensitive information on your personal computer. (Federal Trade Commission 2005).
5. Do not select the option to automatically login or remember identification and authentication information. (Federal Trade Commission 2005).
6. Log out of websites and computers when finished with them. (Federal Trade Commission 2005).
7. Practice good password security techniques. Passwords should be complex in length and composition and devoid of dictionary words. People should have a scheme to remember the password versus writing the password down or storing it on the computer. Passwords and PINs should not be given out to other people.
8. Maintain the security of your computer by practicing activities, such as installing operating system and application patches.

9. Resist social engineering techniques to get your personal information. For example, make sure that the website you are using to conduct online transactions is the actual company versus a dummy website.

10. Be aware of the privacy policies of the companies and institutions that you give your personal information to. (Federal Trade Commission 2005).

11. Make sure that all personal information is properly deleted from technological devices before giving them to other people or disposing of them. (Federal Trade Commission 2005).

Other methods of prevention can also be practiced to help avoid identity theft outside of the digital realm. Frank W. Abagnale, whose exploits and life are depicted in the movie *Catch Me if You Can*, recommends protecting your social security number and periodically examining your credit report as the top two ways to protect our identity information (Abagnale 2004). People may not be able to control what happens to their personal information once it is out of their hands, but computer users can definitely become more vigilant about how they use it on the computer and online.

D. SUMMARY

Identity theft is the misuse of another's personal information and identity. The increase in online activities which involve people's personal identification information means that we need to be more vigilant to attempt to avoid identity theft. The majority of identity theft prevention techniques fall under the realm of basic computer security practices, such as securing one's computer and practicing good password security. Other techniques, such as resisting social engineering, being aware of who is collecting the personal information, and knowing what the information is being used for, are also necessary to protect one's identity. These techniques are incorporated into a CyberCIEGE scenario to help raise computer users' awareness about how to avoid online identity theft.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SCENARIO OVERVIEW

A. SCENARIO STORYLINE

There are several things people can do both online and in the real world to help protect themselves and their identifying information. A goal of this thesis was to narrow down that list of prevention techniques into some essential methods of identity theft prevention from the home user perspective. Once the list was redefined, the challenge became translating it into the educational world of CyberCIEGE.

In order to develop an engaging CyberCIEGE scenario, the narrative must be able to speak to the intended audience, portray the intended educational goals, and provide feedback to the player at appropriate moments. In addition, the storyline should be one that entices the player to persist with the scenario. The Identity Theft scenario uses the popularity of the secret agent/espionage genre and the resurgence of fiber art, such as knitting and crochet, in order to engage the player and allow for some creativity with the narrative. As seen with the success of television shows such as *Alias* and *24*, the secret agent/espionage genre is one that pervades popular culture and can serve to draw the player into the scenario. The crochet aspect of the storyline is used to add dimension to the Sydney Chase character.

The basic storyline is that the player must help the user, Sydney Chase, set up her new home computer so that she is protected from identity theft while conducting online transactions. Sydney Chase is a smart, savvy secret agent for the United States federal government. Sydney has purchased a new computer and wants to email her friends and family and search the web. Since she is on a lot of covert missions and focused on protecting her nation, she is not up to speed on the commonly recommended prevention techniques of identity theft for the home computer user. Between missions, one of the main things Sydney enjoys doing is crocheting presents for her friends and family. Her mobile lifestyle has made Sydney see the potential convenience of being able to maximize her time at home and communicate, research, and purchase products, like yarn, online. In the scenario, Sydney wants to use her computer to find a sweater pattern to crochet and purchase the yarn for the project online.

Due to her line of work, Sydney is aware of the importance of protecting and securing information. If Sydney's identity is stolen, she will have to deal with the cost and time involved in the aftermath of identity theft. Also, it could potentially affect her security clearance and job if someone does something harmful or illegal while impersonating Sydney. The scenario player's main objective is, therefore, to advise Sydney on how to conduct herself while online and how to configure her computer so that she is protected.

B. INTENDED AUDIENCE

The major CyberCIEGE audience is DOD civilian and military personnel. As a result of the directives and policies that DOD employees must adhere to, it is important to be able to provide useful Information Assurance training tools. The Identity Theft scenario can be used to teach the Information Assurance principles related to identity theft prevention to both DOD employees and civilian home users.

With the importance of finding ways to guard against identity theft, the concepts presented in this scenario can be applied to different environments and users. The intended audience of this scenario is both the home computer user and those who will be training others in identity theft prevention techniques. Even though the scenario is set in a home environment, the techniques can also be applied to government and corporate workplaces.

C. EDUCATIONAL GOALS

The main educational goal for this thesis was to provide a training tool that helps both the end user and the Information Assurance instructor demonstrate some main identity theft prevention techniques. In Phase 1, the Connect objective has the player connect Sydney's computer to the router via her local home network. Once this is done, the player is supposed to select the appropriate procedural settings to provide the computer with some basic security and complete the Secure objective. The concept presented to the player at this point is the importance of securing a computer that is connected to the internet. Two main ways to do this is to not run executable email

attachments and to regularly update the antivirus protection on the computer. These settings will help prevent attacks such as viruses, worms, Trojan horses, and trap doors. These attacks can then be used to gain personal information and to steal the user's identity.

In Phase 2, a quiz format is used in order to see how the player would react to a social engineering attack and to another danger of online transactions. The Transact objective in this phase is to answer the questions correctly. The first question relates to conducting online transactions securely. The player should make sure that the browser is using SSL by checking the web address and making sure it is https versus http. The goal here is to get across to the player that when money is transferred online or items are purchased, it is important to make sure the connection is secure. The quiz's second question asks the player to decide what to do when Sydney gets a phishing email. Phishing is when a person receives an email claiming to be from a legitimate source, like eBay or a bank. The email then asks the user to click on a hyperlink to fill in some information on a web form. This question demonstrates the danger of providing personal information to unknown sources.

After playing this scenario, the goal is for the player to gain awareness of behaviors and actions to prevent identity theft. Throughout the game there are also pointers about advanced or extra preventative techniques, such as being aware of companies' privacy policies or only transacting with websites that are well established and familiar. This thesis also added an identity theft section to the CyberCIEGE encyclopedia to assist the player in completing their objectives. This scenario will be able to provide the player with a starting point of the basics of identity theft prevention and make them aware of the dangers that can occur.

D. SCENARIO ELEMENTS

CyberCIEGE has several elements that are used to structure the scenario environment and storyline. The different physical environments of the scenario are distinguished by *zones*. In each zone, there can be *physical components*, such as web servers, computers, and routers. Information, referred to as an *asset*, is stored on physical

components. Virtual users complete *asset goals* by accessing the goal's associated asset. The scenario is also broken up into various *phases* and *objectives*. The player moves to the next phase by completing all of the current phase's objectives. Objectives are usually tasks such as establishing a network connection or incorporating security into a zone or physical component.

The CyberCIEGE game engine has the ability to randomly initiate automatic attacks, such as Internet attacks, and the player has to protect the components from these dangers. Scenario developers can assign *motives* to assets. A motive is a numerical value signifying an attacker's level of motivation for attacking the asset. CyberCIEGE's automatic attacks use the asset's motive to regulate the frequency and amount of attacks it generates. High motive values result in more frequent and complex attacks. The scenario developer also has the ability to create conditions and triggers in order to interact with the player and cause events to occur. Conditions and triggers provide the developer a flexible method to illustrate the scenario's educational goals. Some commonly used triggers are message pop-ups, tickers, and help tips. The Identity Theft scenario uses all of these scenario elements to reach the intended audience, achieve the scenario's educational goals, and implement the scenario's storyline.

1. Sydney's Home Zone

The main environment of the Identity Theft scenario is Sydney Chase's Home. In this zone, there is one computer (Sydney's Computer) and a router from the DSL Company (Bit Flipper Router Home). There is one asset on Sydney's computer, called Sydney's Info, which is composed of the files and other electronic information that resides on Sydney's Computer. This information is susceptible to Internet attacks once Sydney's Computer is connected to the Internet. These attacks are implemented using triggers and CyberCIEGE's attack engine. Sydney's Info has a low motive value assigned to it which allows some of CyberCIEGE's automatic Internet attacks. However, attacks were primarily generated through the use of conditions and triggers. Conditions were used to assess the scenario's state and settings. Triggers were then developed to respond to those conditions. This strategy was chosen to allow for more control and

flexibility in developing a negative feedback mechanism. It also provided a method to assist the player in achieving goals and objectives.

At startup, Bit Flipper Router Home is connected to the Internet and also has a local area network connection for Sydney's Home Network. But, the Home Network cable is not connected to Sydney's computer. This is done so that the player has to make the network connection from Sydney's computer to Bit Flipper Router Home in order to meet the BrowseEmail asset goal. The BrowseEmail asset goal is for Sydney to browse the web and use her web-based email account. It requires the ability to reach the Web Server in the Web zone via the Internet.

Because the goals of this scenario were not related to physical security, Sydney's Home starts out with a key lock, visual inspection, and a poor zone alarm. These physical security components are all reasonable security components for a home environment. These also help defend against some of the physical security attacks built into the game engine.

2. Web Zone

The second zone in this scenario is the Web zone. The physical components in this zone are a Web Server and a router (Bit Flipper Router Web). At startup, the Web zone's network is already connected and working. The Web Server is connected to the Bit Flipper Router Web through a local area network connection. Bit Flipper Router Web is then connected to the Internet.

There is one asset in the Web zone which is Crochet Central's Web Page on the Web Server. Crochet's Central's Web Page is a vast research database of free patterns, tips and news from the crochet community. Sydney needs access to this web page in order to find a pattern for her next crochet project. This asset is associated with the BrowseEmail asset goal. To prevent CyberCIEGE's game engine from generating attacks, a motive value of zero was assigned to the Web Page asset.

Also, the Web zone and its components are secured with strict settings so that the player does not have to deal with automatic attacks from the game engine relating to the Web zone. This is done to keep the focus on Sydney's Home zone.

3. Feedback

The scenario contains feedback in several forms to help the player progress through the scenario. For example, when the player selects wrong or unnecessary settings, feedback is provided to guide the player towards the correct settings. CyberCIEGE has the capability to change the player's budget in order to provide monetary consequences to the player's choices. This scenario does not use this method to educate the player because it did not fit with the home user environment of this scenario. Instead, this scenario uses message, help, and ticker triggers to inform and guide the player through the scenario. These mechanisms try to keep the player focused on the information being presented in the scenario versus dealing with maintaining aspects of CyberCIEGE like budgets. Conditions and triggers are also used to provide attacks and negative feedback to the player.

In the first phase, the main form of feedback is message triggers. If the player does not connect Sydney's computer to the router, the player receives a message saying that the computer can be connected to the router by going to the network screen. The player will receive a message, while on the network screen, if the computer has not been connected after a certain amount of time. After Sydney's computer is connected, the player receives recognition that the BrowseEmail asset goal has been achieved with both a message and ticker trigger. This message signifies that the Connect objective of Phase 1 has been achieved.

In order to satisfy the Secure objective, the player must select both "Regular Antivirus Updates" and "Don't Run Attachments" in the procedural settings window of the Components screen. When the player selects these settings, a message trigger notifies the player about completing Phase 1 and provides directions back to the objectives window to see the objective for Phase 2. If the player chooses only one of the correct settings, a congratulatory message appears which also provides hints about the missing setting.

If the player selects settings that would signify too much, redundant or unnecessary security settings, messages appear to guide the player back in the right direction. When the player has not selected the appropriate settings in a timely manner, a

warning message appears about the dangers of being connected to the internet without any protection. After this warning appears, attacks on Sydney's computer begin until the player chooses the correct security settings. These attacks are driven by conditions and message triggers. The first attack, a virus, occurs when the computer is connected and does not have the "Regular Antivirus Updates" setting. The next attack, a Trojan horse, occurs when the computer is connected and does not have the "Don't Run Attachments" setting. Another attack occurs when the computer is connected and the computer does not have either of the correct security settings. This attack is in the form of a ticker message that emphasizes the danger of not protecting personal information.

The following table delineates the kind of messages that are triggered when certain procedural and configuration settings are chosen by the player.

Setting	Feedback
Automatic Antivirus Updates	This setting could interrupt her computer use and means that the computer would have to be on at specific times, which would be impractical.
No Machine Modifications	Sydney should be able to make changes to her own computer.
No External Software	Sydney should be allowed to install whatever software she wants to on her own computer.
Scan Email Attachments	This setting is redundant because the web-based email service Sydney uses automatically scans email attachments.
Strip Email Attachments	This setting affects Sydney's email functionality such that she will not be able to look at pictures, documents, etc. that people send her.
No Web Mail	This setting would prevent Sydney from having access to her web-based email account.

Table 1. Feedback

In the second phase of the scenario, a quiz format was used to test the player's knowledge about secure browsing and social engineering. A quiz format mimics more closely what occurs in the real world. The player is presented with a situation and has to make a choice to either proceed in a particular way or not. A quiz format also provides the player with an experience different from one associated with message, help, and ticker triggers from the first phase; it allows for a new way of interacting with the scenario.

Feedback can also be found on the various screens in the scenario. On the Objectives screen, the player can see both the list of objectives to be completed and which objectives have already been completed. The screen can also be used to see which phase the player is currently in and how many phases are left in the scenario. The Zone screen has information about the two zones in the scenario, such as physical security, access lists, and the computers in the zones. The component screen details information about the Web Server and Sydney's Computer. On the User screen, the player can see a description of the user and asset goals. The player can also see if there are any asset goal failures by looking at this screen. The Asset Screen details the Web Page and Sydney's Info assets and tells the player the locations of the assets. The scenario takes the player to the Debriefing screen once the game is either won or lost. The player wins by completing the objectives in Phase 1 and answering "no" to both of the questions in Phase 2. The player loses by answering "yes" to either of the questions in Phase 2.

E. SUMMARY

The Identity Theft scenario is intended to be used by DOD and civilian computer users and Information Assurance instructors as a training tool in identity theft prevention techniques. In the scenario, the player must help the user, Sydney Chase, set up her new home computer so that she is protected from identity theft while securely conducting online transactions. The scenario's storyline was implemented using various CyberCIEGE tools and components. After development, the scenario underwent an informal testing process, which is described in the next chapter.

IV. TESTING

A. TEST STRATEGY

To validate that the scenario worked as intended, the test strategy was to identify some test cases based on the scenario's objectives and tasks. These cases were then used to ensure that the expected and experienced results coincided when the player performed either no actions or the wrong ones. A test case for the winning strategy of the scenario was also included. If bugs or unexpected results appeared during testing, the scenario was revised to correct these problems. However, if the problems encountered related to game engine or scenario definition tool issues, then these bugs were informally identified and reported. Since the CyberCIEGE game engine has some randomness associated with its behavior, each test case was run multiple times to insure the scenario reacted as expected each time. Fellow CyberCIEGE developers assisted in the testing by playing the scenario and providing comments and suggestions.

The test strategy for this scenario is informal mainly due to the time and scope of this thesis. However, this method was also chosen due to the evolving nature of the CyberCIEGE game engine and Scenario Definition Tool themselves. During the course of the scenario development, there were several updates to the game engines which included improvements and error corrections. This scenario was tested with the latest version of the CyberCIEGE game engine, version 1.4k. This version of CyberCIEGE changed the wording of the "Don't Run Attachments" procedural setting to "Beware of Email Attachments."

B. SCENARIO TEST CASES

The following are test cases breaking the scenario down into its three objectives and testing what happens when the player follows certain playing strategies.

1. Test Case 1: Winning Strategy

To successfully complete the scenario, the player must complete Phase 1 and answer both of the questions in Phase 2 correctly. Phase 1 is completed by first

connecting Sydney's computer to her router through her Home network. To do this, the player first switches to the Network screen by selecting the Network tab. The connection is made by selecting Sydney's computer and then selecting the Home Network connection. Then, in either order, the player chooses both the "Don't Run Attachments" and "Regular Antivirus Updates" from the procedural settings on the Component screen. These actions complete both the Connect and Secure objectives that make up Phase 1.

In Phase 2, the Transact objective quizzes the player on responses to social attacks. The first question deals with secure browser connections and online transactions. By answering "no" to this question, the player encourages Sydney to be cautious of her online transactions and emphasizes the importance of using secure connections when buying things online. Next, the player should instruct Sydney to be cautious of phishing emails requesting personal information and answer "no" on the second question. This action successfully completes both the Transact objective and the scenario itself. The player is then presented with the winning Debriefing screen.

2. Test Case 2: Connect

The Connect objective is met when Sydney's computer is connected to her router through her Home Network cable. Since there is only one way to connect the computer to the router, this test case examines what happens when the player does not connect Sydney's computer to the home network. It also makes sure that the player can not change any of the initial network connections.

Since the goal of this scenario is to educate and instruct the player, guidance appears to help move the player along when the objective has not been completed in a certain amount of time. If the player does not connect the two components after a certain amount of time, a help tip appears that directs the player to the objectives screen in order to get advice on where to start. The player also encounters a help tip providing information about pressing the play button to pause and play the scenario.

When the player is on the network screen and is having trouble completing the objective, help appears to guide them in connecting the two components. If the player clicks on any combination of network cables and components other than the winning

combination, no other connections can be made or taken away. For example, the components in the Web Zone were made static, so that the player can not change the network connections of that zone.

3. Test Case 3: Secure

The Secure objective is completed when the player selects both the "Don't Run Attachments" and "Regular Antivirus Updates" procedural settings. This test case examines what happens when the wrong settings are chosen for Sydney's computer. It also tests what happens when the player does not select any security settings for Sydney's computer.

When the player has not selected the appropriate settings in a timely manner, a warning appears about the dangers of being connected to the internet without any protection. After this warning appears, attacks on Sydney's computer begin until the player chooses the correct security settings.

One part of the Secure objective is to select the "Regular Antivirus Updates" setting for Sydney's computer. The "Automatic Antivirus Updates" procedural setting is the wrong choice for this part of the objective. If the player selects this setting, the scenario notifies them that this would be problematic and directs them to the correct setting.

Another component of the Secure objective is to have the player instruct Sydney to be cautious about email attachments by selecting the "Don't Run Attachments" procedural setting. The wrong settings for email attachment protection would be the "Scan Email Attachments" and "Strip Email Attachments" configuration settings. If the player selects one of these settings, an appropriate message appears explaining why that settings is not appropriate or necessary.

This test case also tests what can happen when unnecessary procedural settings are selected. If the player selects either the "No Machine Modifications" or "No External Software" settings, messages appear reminding the player that the computer is Sydney's personal computer and she should be able to make these kinds of alterations. The player

will also encounter a message if the “No Web Mail” setting is selected, because this would interfere with Sydney’s ability to use her web-based email account.

4. Test Case 4: Transact Quiz

The Transact objective is met by successfully completing a quiz. This test case deals with testing whether or not the quiz responds correctly when the player answers the questions incorrectly. If the player answers “yes” to both of the question, Sydney’s identity is stolen. The player is then presented with the losing Debriefing screen. If the player answers “yes” to one of the questions and “no” to the other one, the player still fails the quiz and the losing Debriefing screen is shown.

5. Results

Except for one test case, all the expected results and experienced results coincided. The unexpected result came while testing the quiz in Test Case 4. If the player does not press either of the keyboard responses and only clicks “OK” on the question window, the game engine recognizes this as a “no” response and proceeds accordingly. This means that the player can successfully complete the quiz by just selecting the “OK” button on the question window. This result is due to a SDT (Scenario Definition Tool) issue with the register condition’s default setting and has been reported as a problem.

While completing the test cases for Phase 1, there was one unexpected result which was not covered by the test cases. If the player completed the Secure objective before completing the Connect objective, the scenario proceeded on to Phase 2. This undesirable result was solved by making some changes to the scenario preventing the player from moving to Phase 2 until both Phase 1 objectives are met.

After testing, some refinements were also made to the text that appears in the screens and messages that appear throughout the game. This was done to attempt to find the most effective word choice for the player. When necessary, there were also some changes to the timing of the various text pop-ups or tickers in order to improve the player’s experience.

C. CYBERCIEGE TESTING

The CyberCIEGE game engine and SDT (Scenario Definition Tool) are both currently under development. As a result, this thesis also provided an informal testing of these components. Whenever problems were encountered that related to the game engine or SDT, an informal approach was taken to identify and report problems and to make improvement suggestions.

1. Invisible Users

In the beginning of the scenario development, there was an issue with the user being invisible. The user was present on the screen, according to the speech pop-ups, but the graphic for the user was not being displayed. This was a game engine problem that was resolved by removing a problematic optimization in the source code.

2. Multiple LAN connections

When working on the Connect objective portion of the scenario, it seemed to be confusing to have only one of the network connections displayed around the given component at a time. Originally, a component with multiple network connections would only display one of the connections around it in a colored box. This situation arose only when the component in question was the only component on the network. However, after identifying this as a user interface problem, the game engine was revised to allow for multiple boxes to appear around the component. Now, when the player initially goes to the Network screen, the router has both red and green boxes around it depicting the router's Home Network and Internet connections.

3. Colons and Backslashes

The SDT does not allow the combination of a colon and backslashes to appear in a text field. This problem was discovered when trying to input the text for the question trigger dealing with secure browsers. The text originally had the "http://www.yarnbarn.com" and "https://www.yarnbarn.com" as a part of the first question on the quiz. CyberCIEGE crashed when this question trigger fired due to the

colon and backslash combination. To resolve this issue in the scenario, the question's text was changed in order to avoid this problem. The SDT's issue with colons and backslashes has been reported.

4. Register Condition

When testing the quiz portion of the scenario, a problem with the register condition was identified. It appears that the default for the key register condition is "1" or "no" in the SDT. This is a problem, because if the user clicks on the OK button without inputting a "no" or "yes" response, the game engine reacts as if the user selected "no". Since successful completion of the quiz in Phase 2 depends on answering "no" to both of the questions, this bug can allow the user to win the scenario without entering the correct responses. This problem was reported and resolved by changing the key register condition values from "1" and "2" to "n" and "y."

5. Camera Drifting

When CyberCIEGE starts and the camera is repositioning to the home office site, the camera panning is interrupted if the player makes any mouse movements or clicks. This causes the camera to stop where it was interrupted. This looks like a problem with the game engine and is especially noticeable on slower computers. This problem has been identified and reported.

6. Paragraph Formatting

When composing messages that appear to the player, it is helpful to be able to insert formatting to the messages by using tools such as paragraph markers. This can be accomplished by inserting (PARAGRAPH) in the position where the paragraph marker should exist. However, it was found that this formatting is only available for triggers such as message and question triggers. When placed in the message box for triggers such as SetPhase, (PARAGRAPH) will just be treated as a part of the text and not a paragraph marker. This problem has been identified and reported.

D. SUMMARY

The Identity Theft scenario worked as expected and any bugs encountered along the way were either reported or resolved. During both the development and testing of the scenario, recommendations and suggestions for improving the Identity Theft scenario, CyberCIEGE game engine, and SDT emerged. These recommendations are discussed in the next chapter along with suggestions of how the Identity Theft scenario can be utilized.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. SCENARIO APPLICATIONS & EXTENSIONS

Multiple environments exist where the Identity Theft scenario could be applied. As an educational training tool, the scenario could be used as a part of introductory Information Assurance courses in an academic setting. It would also work well as a part of on-the-job Information Assurance computer training in both government and corporate environments. For example, DOD employees are mandated to complete computer Information Assurance training annually. This scenario could be used as a part of such training. The scenario is also short enough that it could also be used on the lecture circuit so that the presenter has a visual example for the audience when discussing issues such as identity theft or Information Assurance. Home computer users could come into contact with the scenario if it was incorporated as part of the software bundle that comes with a new computer or available as a download.

Since this scenario deals with basic identity theft prevention techniques, more extensive scenarios dealing with identity theft prevention could be created in the future. Attackers are going to continue to derive new methods to steal information, which means that users will need to be informed of new prevention techniques. One possible future scenario could explore how identity theft prevention can be accomplished in the wireless domain. By making the local area networks in the scenario wireless, this could bring in new issues and prevention mechanisms to explore in CyberCIEGE. Also, since wireless internet is becoming more widespread in homes and businesses, this could become a more relevant network setup for the Identity Theft scenario. Another future scenario could deal with applying these prevention techniques to handheld mobile computing devices, such as PDAs and cell phones. Both of these future scenarios would bring wireless and mobile security issues into CybeCIEGE. As a result, there may need to be some additions to the game engine in order to allow wireless networks and handheld mobile devices.

The Identity Theft scenario could also be improved by providing some multimedia feedback, such as sound and movies. For example, a movie clip could

emphasize one of the internet attacks made on Sydney's computer when it does not have the proper procedural settings selected. This would make the danger more imminent to the player and add to the overall experience. It would also be interesting to have a movie clip available if the player loses the game. The clip could display someone stealing the information and using it to cause harm to Sydney. Another clip could play when the player wins the game. This clip would be celebratory and would contain information not covered in the scenario, such as tips on setting up a personal firewall.

Since the goal of this thesis was to focus on the essential and basic prevention techniques, future versions of the scenario could integrate additional problems, tips, and information. Spyware could be added to the possible attacks on Sydney's computer. For example, an attacker could install some spyware on the computer in order to gain her personal information. Information relating to properly deleting information from computing devices before giving or throwing the devices away could also be incorporated. Another aspect which could be added to the scenario is information on what to do to recover from identity theft. This could either be added at the end of the scenario as a movie clip or as a part of the debriefing screen.

Due to the scope and timeframe of this thesis, an informal testing process was conducted. However, it would be useful to conduct a more involved and formal testing process. The scenario should be tested on users with varying levels of computer experience and Information Assurance knowledge. Groups of testers should test the scenario from the end user, instructor, and employee perspectives respectively. A more rigorous testing process should also be conducted to make sure that all bugs are found and resolved. When versions of CyberCIEGE are released in the future, the scenario should also be tested to make sure game engine changes and additions do not affect or change the scenario's behavior in unexpected ways.

B. CYBERCIEGE RECOMMENDATIONS

The game engine attacks and options in the SDT are geared mainly for the corporate or military environment scenarios. The Identity Theft Scenario was the first to be set in a home environment. The graphic for the offsite office was used to depict

Sydney's home, but it might be useful in the future to have more zone graphics available to the scenario developer. When designing a scenario, it would also be useful to have more choices in the user graphics. Initially, the user for the Identity Theft scenario was the player's Great Aunt. This storyline was eventually changed for several reasons. One reason was that CyberCIEGE's female user graphic is that of a young woman. Therefore, the older woman user description would not match very well with the female graphic available. As with the zone graphics, having more options of user graphics makes the development process easier and allows for more creativity and options.

Another aspect which would improve the scenario development process is for the SDT to either have a new and different user interface or for there to be more flexibility within the current one. For example, in order to make changes to the user's name, it would help to have one place to change the name and have the change propagate to elsewhere in the scenario. When the scenario storyline switched from the Great Aunt to Sydney Chase, there were several places where the changes had to be made. If the SDT interface was designed to make changes easier, the storyline switch would have been easier to implement. Although, the automatic nature of the attacks and thoughts are very useful for some scenarios, most of the game engine's automatic responses did not apply to the home user environment of the Identity Theft scenario. Therefore, it would be useful for the developer to have the option in the SDT interface to switch off the game engine's automatic thought and attack triggers.

Currently, the main way to interact with the player is through text-based windows and pop-ups. Another CyberCIEGE recommendation would be to include more multimedia options for the developer to use. For example, speak triggers could be done with an audio file versus a pop-up message. If other communication techniques were added to CyberCIEGE, the overall playing experience would be improved and the developer would have more tools to create interesting and engaging scenarios.

Finally, the development process would be greatly improved if the SDT had an improved method of debugging the scenario. Currently, there is a crash text document and a log file to assist in error correction. But, the development process would be vastly

improved if there was a clearer method of notifying the developer where the errors exist and how to correct the errors.

C. CONCLUSION

This thesis contributes to the current CyberCIEGE Information Assurance training suite and aids in the improvement of the CyberCIEGE game engine and scenario definition tool. The Identity Theft scenario can be used as a training tool for both the end user and the Information Assurance instructor. User awareness and training are the main tools to lessen the danger of identity theft. This scenario provides some basic identity theft prevention techniques so the player can learn to keep identifying information safe while online. It can also be used to provide a real world example of why basic Information Assurance concepts, such as antivirus protection or email security, are important to combating online dangers. After scenario development, an informal test process of the Identity Theft scenario was conducted. Testing found that the experienced and expected results coincided. Recommendations for improvement of the CyberCIEGE game engine, Scenario Definition Tool, and Identity Theft scenario were also provided.

LIST OF REFERENCES

Abagnale, Frank W. "14 tips to avoid identity theft." 8 December 2004. Available from http://www.bankrate.com/brm/news/advice/20030124b.asp Accessed 7 June 2005.

BBC News UK Edition. "Passwords revealed by sweet deal." 20 April 2004. Available from http://news.bbc.co.uk/1/hi/technology/3639679.stm Accessed 3 April 2005.

Caloyannides, Michael A. "The Cost of Convenience: A Faustian Deal." *IEEE Security & Privacy*, March/April 2004, 84-87.

Denning, Dorothy. *Information Warfare and Security*. Boston: Addison-Wesley, 1999.

Federal Trade Commission. "ID Theft: What's It All About." Available from http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm Accessed 30 March 2005.

Irvine, Cynthia E, Michael F. Thompson, Ken Allen. "CyberCIEGE: Gaming for Information Assurance," *IEEE Security & Privacy*, May/June 2005, 61-64.

Ostrom, Mary Anne. "Protect Passwords? Not if latte is free." 6 May 2005. Available from http://www.mercurynews.com/mld/mercurynews/business/11578776.htm Accessed 6 May 2005.

Synovate. "Federal Trade Commission-Identity Theft Survey Report." 3 September 2003. Available from http://www.ftc.gov/os/2003/09/synovatereport.pdf Accessed 30 March 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX - CYBERCIEGE ENCYCLOPEDIA PAGE

The following is the text that appears on the “What is Identity Theft?” section of CyberCIEGE’s encyclopedia.

Identity theft is the misuse of one's personal information and identity. The increase in online activities which involve people's personal identification information means that we need to be more vigilant to attempt to avoid identity theft. The majority of identity theft prevention techniques fall under the realm of basic computer security practices, such as installing regular antivirus updates and being cautious of executable email attachments. Other techniques, such as resisting social engineering, being aware of who is collecting the personal information, and knowing what the information is being used for, are also necessary to protect one's identity.

A victim's personal information can be used for both financial gain and to physically misrepresent the victim to people such as law enforcement officials, employers or medical providers. The amount of time associated with resolving the problems that arise in the aftermath of identity theft should also be considered a cost of identity theft.

Not only does identity theft impact the consumer, but it also negatively affects businesses and banks. Businesses and financial institutions have had to keep up with the increase in identity theft by developing new services. For example, most credit card providers now provide the option of placing the credit card owner's picture on the credit cards for authentication purposes. Similarly, since monitoring one's credit report is a commonly recommended technique to prevent identity theft, some financial institutions now allow consumers to buy identity theft prevention each month through special credit checking services.

Social engineering is a key way that personal information is collected for misuse. People give away their contact information, date of birth, credit card number, and social security number for lots of reasons and services these days. This personal information is asked for in conjunction with online activities that range from buying books to joining a professional organization to paying bills.

Even if key information, such as passwords, is not supplied by the individual, enough personal information can be collected to be damaging to the security of a person's identity. It is important to be aware of who exactly is collecting personal information, what the information is going to be used for, and what the privacy policies are of the companies who have the information.

The following is a breakdown of commonly recommended methods of prevention for digital identity theft:

-Install and regularly update antivirus and spyware protection software.

-Be cautious about executing email attachments. This is a common way that attackers can install malware and spyware on the computer.

-Use a secure web browser for online transactions which employs techniques, such as encryption, to keep your personal information more secure.

-Resist social engineering techniques to get your personal information. For example, make sure that the website you are using to conduct online transactions is the actual company versus a dummy website.

-Practice good password security techniques. Passwords and PINs should not be given out to other people.

-Maintain the security of your computer by practicing activities, such as installing operating system and application patches.

-Install and properly configure a firewall on your personal computer.

-Be aware of the privacy policies of the companies and institutions that you give your personal information to.

-Make sure that all personal information is properly deleted from technological devices before giving them to other people or disposing of them.

This Federal Trade Commission web page describes the basics of identity theft and what people should do if they become an identity theft victim. This Federal Trade Commission Survey Report from 2003 describes the forms of identity theft and provides some identity theft statistics.

People may not be able to control what happens to their personal information once it is out of their hands, but computer users can definitely become more vigilant about how they use their information on the computer and online.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Ken Allen
   Rivermind, Inc
   Mountain View, CA

4. Hugo A. Badillo
   NSA
   Fort Meade, MD

5. George Bieber
   OSD
   Washington, DC

6. RADM Joseph Burns
   Fort George Meade, MD

7. John Campbell
   National Security Agency
   Fort Meade, MD

8. Deborah Cooper
   DC Associates, LLC
   Roslyn, VA

9. CDR Daniel L. Currie
   PMW 161
   San Diego, CA

10. Louise Davidson
    National Geospatial Agency
    Bethesda, MD

11. Vincent J. DiMaria
    National Security Agency
    Fort Meade, MD

12. LCDR James Downey
NAVSEA
Washington, DC

13. Scott Gallardo
Rivermind, Inc
Mountain View, CA

14. Dr. Diana Gant
National Science Foundation

15. Jennifer Guild
SPAWAR
Charleston, SC

16. Richard Hale
DISA
Falls Church, VA

17. LCDR Scott D. Heller
SPAWAR
San Diego, CA

18. Wiley Jones
OSD
Washington, DC

19. Russell Jones
N641
Arlington, VA

20. David Ladd
Microsoft Corporation
Redmond, WA

21. Dr. Carl Landwehr
National Science Foundation
Arlington, VA

22. Steve LaFountain
NSA
Fort Meade, MD

23. Dr. Greg Larson
IDA
Alexandria, VA

24. Penny Lehtola
NSA
Fort Meade, MD

25. Gilman Louie
In-Q-Tel
Menlo Park, CA

26. Ernest Lucier
Federal Aviation Administration
Washington, DC

27. CAPT Deborah McGhee
Headquarters U.S. Navy
Arlington, VA

28. Dr. Vic Maconachy
NSA
Fort Meade, MD

29. Doug Maughan
Department of Homeland Security
Washington, DC

30. Dr. John Monastra
Aerospace Corporation
Chantilly, VA

31. John Mildner
SPAWAR
Charleston, SC

32. Jim Roberts
Central Intelligence Agency
Reston, VA

33. Keith Schwalm
Good Harbor Consulting, LLC
Washington, DC

34. Charles Sherupski
Sherassoc
Round Hill, VA

35. Dr. Ralph Wachter
ONR
Arlington, VA

36. David Wennergren
DoN CIO
Arlington, VA

37. David Wirth
N641
Arlington, VA

38. Daniel Wolf
NSA
Fort Meade, MD

39. Jim Yerovi
NRO
Chantilly, VA

40. CAPT Robert Zellmann
CNO Staff N614
Arlington, VA

41. Dr. Ernest McDuffie
Office of Naval Research
Arlington, VA 22203

42. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, CA

43. Paul C. Clark
Naval Postgraduate School
Monterey, CA

44. Michael Thompson
Naval Postgraduate School
Monterey, CA

45. Carrie Ruppar
Civilian, Naval Postgraduate School
Monterey, CA